

Cyber Services

Service Category: Security Services, Cloud Support Services

About Our Service

Frazer-Nash delivers comprehensive cyber services to empower organisations to secure and manage cloud and enterprise technologies in an evolving threat landscape. Our expertise spans enterprise architecture, socio-technical assessments, technical assurance and compliance as well as post-quantum cryptography and AI security. Our strategic guidance enables organisations to achieve long-term resilience.



Service Features

Cyber strategy and governance for cloud-enabled business systems and organisations

Systems-based engineering approach to solve complex challenges

Model-based approach to enterprise and technical architecture

Enable transformation of technology e.g. post-quantum cryptography and AI security

Socio-technical system analysis to understand threats, vulnerabilities and risks

Technology strategies and roadmaps to streamline migration plan

Communications, network and information systems design and assurance

Installation security and accreditation of secure facilities

Data analytics and modelling to optimise decision-making and risk mitigation

Supply chain security analysis and assurance

Service Benefits

Increase confidence
in managing cyber
risks and
compliance
obligations

Improve decision
capacity with
robust, transparent
and actionable
insights

Reduce expenditure
using systems and
models to solve
complex challenges.

Efficient design of
services and
business through
architectural design

Improve mitigation
of cyber-related
threats to your
business

Adopt a flexible and
agile approach to
information
assurance

Improve confidence
in supply chain
security

Empower your
workforce with
transferred skills
and knowledge

Achieve Secure by
Design principles

Accelerate
transformation to
new technologies
with security and
resilience

Detailed Service Definition

What is cyber?

The term or prefix 'cyber' is now used extensively in business, industry, government, law and policy where it is widely accepted as providing a reference to the virtual (i.e. other than physical) world created by the internet and other electronic communications systems and services. Cyber is often used as a prefix to form words relating to the existence or provision of this virtual world, such as 'cyberspace', however their meaning and context can vary significantly between, and within, governments, departments, organisations and even within the cyber industry itself.

Detailed Service Definition (continued)

Our cyber offering

At Frazer-Nash, we believe that cyberspace can be viewed as a global domain within the information environment where entities interact. As such it may be considered to consist of the virtual environment formed from, or enabled by, information services (including cloud services), and the interdependent networks of information technology infrastructures on which these services run, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. We consider the demands of operating within cyberspace holistically, not just from a technology perspective, but also considering people and processes.

We recognise the need to understand our client's view of the different aspects of cyber and, with our extensive service offerings within this domain, can tailor our services to meet their individual, and often unique, requirements.

Detailed Service Definition (continued)

The range of services we can include in this domain is extensive and includes:

Cyber Strategic Advice – Providing advice across all levels of an organisation supporting strategy, vision and policies on the threats to data and assets and how to protect them from cyber-attacks: considering people, processes, information, technology and facilities.

Cyber Systems Engineering – This is a robust approach to the design, creation and operation of information systems. This consists of the identification and qualification of user needs and requirements, creation of alternative system design concepts, design trades, selection and implementation of the best design, verification that the design is properly built and integrated and post implementation assessment of how well the system meets (or met) the user needs. This also includes the principles of Secure by Design to ensure systems are built securely and sustainably for the expected life of the system and in accordance with the desire risk appetite;

Detailed Service Definition (continued)

The range of services we can include in this domain is extensive and includes:

Cyber Systems Architect – This provides the knowledge and skills across the development and acquisition lifecycles to provide environments which require high levels of information security. This covers the principles of information protection, and the role application technology has in meeting the goal of information protection, supporting the build and design of architectures to manage risks and the operation and management of developed systems. A key consideration in developing a cyber system is the devolving of capability to a services-based architecture of which the cloud is a key component. This can include the design or development of a wider-business Target Operating Model to incorporate the cyber resilience, which alongside technology changes can identify wider-changes needed like training, develop and organisational restructuring and policy changes to achieve business outcomes.

Cyber Vulnerability Investigation/Analysis – This provides a detailed understanding of an organisation's cyber domain, reducing the likelihood and impact of potential threats, increasing an organisation's cyber awareness, providing cyber security advice and advising on potential architectures including hosting capability in the cloud. This may include undertaking an audit for an organisation against a defined threat. This could lead to a detailed assessment where human factors, facilities, information security (INFOSEC), penetration (PEN) testing, and wider subject matter expert (SME) support is required.

Detailed Service Definition (continued)

Communications/Network Design – Planning and designing complex information and communications networks, covering all technologies across both private and public sector networks, accommodating traffic intensity, load and devolving capability to the cloud.

Data Analytics/Modelling – Data analytics is the science of examining raw data with the purpose of drawing conclusions about that information. Data modelling allows the overall analysis to be presented in a format that is meaningful to everybody. Using both aspects across all areas of the business can enhance decision-making and rapidly provide insight to inform business decisions, proactively implement cyber security controls to stay within risk appetite or identify emerging trends or issues.

Facilities/Communications Installation Security/IAM – To provide consultancy for the protection of data and assets within buildings or rooms and associated support infrastructure. Understanding installation, Electro-Magnetic Capability (EMC), Information & Communications Technology (ICT), power, through to electronic security, Wi-Fi, Bluetooth Low Energy (BLE) and control structure and procedures. Drawing on Site Coordinating Installation Authority (SCIDA) and TEMPEST Control Officer (TCO) expertise.

Detailed Service Definition (continued)

Information Security/Assurance – INFOSEC consultants provide best practice advice and documentation for resilient systems to provide mitigations for any compromises in the confidentiality, integrity and availability for information systems. This can also encompass the wider-supply chain audit or assessments covering cyber security standards and integrity expected, and the resilience of the supply chain to different cyber risks

Why Frazer-Nash Consultancy?

Frazer-Nash Consultancy is an independent engineering and technology consultancy with over 35 years' experience delivering high-quality digital and cloud-enabled solutions. We support organisations operating in complex and regulated environments through our collaborative approach and deep expertise in digital engineering, software development and systems integration.

We are **solution and technology-agnostic**. We assess our clients' requirements and provide impartial advice and design solutions based solely on their needs. This independence enables us to select the most appropriate cloud technologies and architectures to deliver secure, resilient and value-for-money outcomes.

Our cloud solutions are informed by experience gained across multiple platforms, sectors and use cases. We combine proven engineering discipline with a strong understanding of integration and whole-system design to support and enable cloud adoption while managing risk and ensuring long-term sustainability.

Our Commitment to Quality

Frazer-Nash is committed to delivering consistently high-quality services and outputs that **often exceed customer expectations**. Quality is embedded throughout our ways of working, from engagement and communication through to delivery and assurance.

We actively monitor progress using our robust, proportionate controls, ensuring key decisions are subject to appropriate challenge. Each project is allocated a dedicated Project Manager, a Project Supervisor who independently reviews and approves monthly reports, and a Project Auditor for ongoing quality assurance.

We ensure accuracy and suitability for purpose of all deliverables, with independent verification by two reviewers. Our Quality Management System is certified to **ISO 9001 and TickITplus** (for software development), providing customers with confidence that our quality standards are externally assured and continuously maintained.

Our Security

Frazer-Nash operates robust security processes and controls suitable for handling sensitive and classified information **above OFFICIAL** up to and including **Top Secret**. Security is embedded across our people, processes and systems, ensuring information is protected throughout delivery.

We support sensitive and critical programmes across government and national infrastructure by applying strict information-segregation controls, including team separation to address security, or conflict-of-interest considerations

All 1500 staff hold **BPSS clearance as a minimum**, with the majority cleared to **SC** and over 225 consultants holding **DV clearance**.

Our IT systems are certified to **ISO 27001 and Cyber Essentials Plus**, providing assurance that information security risks are proactively managed in line with recognised industry standards.

Our Approach to Subcontracting

Frazer-Nash primarily delivers services through our large base of permanent staff, supplementing this capability where required with trusted partner organisations to provide additional flexibility, specialist expertise and scale while retaining full delivery control.

We are experienced in engaging and managing subcontractors across the full project lifecycle, ranging from sole traders to large multinational organisations. Our structured approach ensures the right supplier is selected for each requirement and integrated effectively into the delivery team.

Our subcontracting processes focus on robust supplier identification and assessment, clear definition of scope, appropriate flow-down of contractual terms and conditions, and proactive risk management. All subcontractors are subject to proportionate commercial and technical due diligence to ensure they meet our standards for security, quality and delivery, enabling us to deliver outcomes on time, within budget and to the required quality.



Resourcing

Frazer-Nash employs over **1,500 technical specialists** across all grades, from **Follow to Set Strategy**, providing depth, continuity and scalability across a wide range of disciplines, backgrounds and experience levels.

To support agile and flexible delivery, our people are organised into defined **technical delivery areas** (including Information Systems, Cyber, Modelling and Software), which are deployed across multiple sectors such as central and local government, policing, health and energy. This structure, combined with strong portfolio, programme and project management (P3M), enables us to actively monitor demand and adapt resourcing throughout the project lifecycle.

We deliver complex requirements efficiently, consistently and at pace by forming tailored, multi-disciplinary teams led by a single accountable Project Manager.

Our consultants regularly work across different sectors, enabling us to cross-pollinate ideas, tools and best practice between domains. Drawing on in-house expertise, such as information security and human factors, we ensure effective and responsive delivery for every client.



Our Commercial Approach

Frazer-Nash adopts a flexible and transparent commercial approach to ensure best value and a model that aligns to each client's specific requirements. We collaborate with customers to clearly define the scope of services and agree a commercial structure that is predictable, proportionate and aligned to your required outcomes and effective delivery.

Depending on the requirement, this may include a **fixed-price model for clearly defined scopes**, or **time and materials using agreed day rates** where flexibility is required to accommodate evolving needs.

For longer-term or ongoing service requirements, and where we have control over resource flexibility, we can also offer a **single blended day rate** covering a range of grades. This provides simplicity, transparency and ease of management while maintaining access to the appropriate skills at the right time.

Next Steps

To discuss your requirements in more detail or request an order for services, please contact ccs@fnc.co.uk

